



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/785,849	02/16/2001	Hans Christopher Sowa	CM04816H	2108
22917	7590	06/01/2006	EXAMINER	
MOTOROLA, INC. 1303 EAST ALGONQUIN ROAD IL01/3RD SCHAUMBURG, IL 60196			BLUDAU, BRANDON S	
			ART UNIT	PAPER NUMBER
			2132	

DATE MAILED: 06/01/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary

Application No.

09/785,849

Applicant(s)

SOWA ET AL.

Examiner

Brandon S. Bludau

Art Unit

2132

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 13 March 2006.
- 2a) ☒ This action is **FINAL**. 2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-22 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-22 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on _____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
a) ☐ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. _____.
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- 1) ☒ Notice of References Cited (PTO-892)
- 2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
- 3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date _____
- 4) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date: _____
- 5) ☐ Notice of Informal Patent Application (PTO-152)
- 6) ☐ Other: _____

DETAILED ACTION

1. This action is in reply to amendment filed on March 13, 2006. Claims 1-12, 14 and 18-19 have been amended. Claims 1-22 are pending.
2. The examiner withdraws the 112 rejection pertaining to claim 20, as the claim has been properly amended to overcome the previous rejection.

Response to Amendment

3. The amendment filed March 13, 2006 is objected to under 35 U.S.C. 132(a) because it introduces new matter into the disclosure. 35 U.S.C. 132(a) states that no amendment shall introduce new matter into the disclosure of the invention. The added material which is not supported by the original disclosure is as follows:
4. Claim 1, lines 2-3: "a first encryption key associated with traffic encryption for group communications". Paragraph [0045] states that the GCK, which is the first encryption key is "never used for the actual encryption of traffic as it is considered a long term key".
5. Claim 1 line 5: forwarding the key "to a second system device other than a mobile station". Paragraph [0026] discusses the KMF generating the GCK for distribution in the system. A mobile station is considered part of the system, and nowhere in the disclosure is such a negative limitation found that explicitly states the exclusion of a mobile station from being the second device. Furthermore, the Examiner asserts that the action of forwarding to a second device doesn't necessarily demand the second device be the next "hop" in the system.

6. Claim 1 line 10: "forwarding the second encryption key to a third system device other than a mobile station". Paragraph [0071] discloses that the second key is stored at the MS (mobile station), thus it is necessary for this key to have been forwarded to the mobile station.

7. The same arguments apply to the similar amendment to claims 2, 10 and 11 in regards to the limitation precluding the forwarding to a device other than a mobile station.

Applicant is required to cancel the new matter in the reply to this Office Action.

Response to Arguments

8. Applicant's arguments filed March 13, 2006 regarding the forwarding of the keys to a device other than a mobile station in Independent claims 1 and 2 have been fully considered but they are not persuasive. The Roelofsen reference discusses forwarding the keys from the network to the MS, however, as is understood in the art and as is evident in Figure 3 on page 47, the process of forwarding the keys includes a step in which the key is passed to another network element that is not the mobile station, wherein the forwarding to the mobile station is the end destination.

Applicant's arguments with respect to claims 1 and 2 in regards to the third system device being one other than the first and second system devices have been considered but are moot in view of the new ground(s) of rejection. See rejection below.

9. Applicant's arguments with respect to the dependent claims have been considered but are moot in view of the new ground(s) of rejection as applied to the independent claims.

Claim Rejections - 35 USC § 112

The following is a quotation of the first paragraph of 35 U.S.C. 112:

The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

10. Claims 1,2,10,11 are rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the written description requirement. The claim(s) contains subject matter which was not described in the specification in such a way as to reasonably convey to one skilled in the relevant art that the inventor(s), at the time the application was filed, had possession of the claimed invention. See discussion of new matter above.

The following is a quotation of the second paragraph of 35 U.S.C. 112:

The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

11. Claims 1 and 2 rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention. The limitation of the first encryption key being *associated* with traffic encryption is unclear. In the specification the Applicant states in paragraph [0045] that the key is not used for traffic encryption. The metes and bounds of the term “associated with” as applied to the encryption key are unclear.

Claim Rejections - 35 USC § 103

12. Claims 1-4,6-8,10-18, 21 are rejected under 35 U.S.C. 103(a) as being unpatentable over Roelofsen, and further in view of Tiedemann (US Patent 6381454).

As per claim 1, Roelofsen discloses a method comprising the steps of:

Generating, by a first system device, a first encryption key associated with traffic encryption for group communications;

Forwarding the first encryption key from the first system device to a second system device other than a mobile station (page 50 paragraph 8 wherein the first encryption key is the Group Cipher Key (GCK) and the second system device is some network element as referenced in figures 3 and 5);

Generating a second encryption key associated with traffic encryption for group communications by combining the first encryption key with a third encryption key (page 51 paragraph 2);

but does not disclose:

Storing the first encryption key at the second system device, and

Forwarding the second encryption key to a third system device other than a mobile station and other than the first and second system devices.

Tiedemann does disclose a communication infrastructure that stores the first encryption key at a second system device and forwards a second key to a third system device other than a mobile station and other than the first and second system devices (column 14 lines 42-50 wherein the second and thirds system devices are the HLR and the MSC).

Tiedemann is analogous art because it is directed towards an over the air service programming method and infrastructure.

It would have been obvious for one of ordinary skill in the art to modify Roelofsen to include second and third system devices other than a mobile station that store and forward keys.

Motivation for one of ordinary skill in the art to modify Roelofsen would be to enable a system device other than the mobile station to employ voice privacy and message encryption as discussed by Tiedemann (column 14 lines 48-50).

Tiedemann does not disclose that the second system device generates the second encryption key. However, Roelofsen discloses wherein "the common cipher key is generated by the SwMI and distributed to the MSs... and is used to set up a group call with all MSs that at the moment are in a certain area." From this it would be evident by one of ordinary skill in the art that some network element that controls an area such as a switching center or base station must be in control of the CCK and since the second key is generated by combining the first key (GCK) and the third key (CCK) (page 51 second paragraph) it would be obvious to one of ordinary skill that this key would be generated by the element that controls the specific area (a second network element). Roelofsen doesn't specifically disclose the elements in the SwMI, but from figure 3 it is obvious that there is a second or third element other than a mobile station in the infrastructure. And further, in view of Tiedemann, it is evident that similar infrastructure is common in the art that includes multiple network elements that are responsible for storing and forwarding keys.

13. Claim 2 is rejected because it discloses the same subject matter as claim 1. The switching of the first system device to the second system device doesn't change the

scope or limitations to the claim. The claim is the same wherein now the first system device is one of a network element such as the (HLR or VLR or MSC as cited in claim 1) and the second system device is the authentication center).

14. As per claim 3, Roelofsen discloses the method of claim 1, wherein the third system device is any of a base station, a base site, and TETRA site controller (page 50 paragraph 5 wherein the Derived Cipher Key is used for uplink communications, thus implying the DCK is at the network, i.e. base station), wherein the step of forwarding the second encryption key to a third system device is triggered by a mobile station residing at any of the base station, the base site, and the TETRA site controller when the first encryption key is generated (page 50 paragraph 5 wherein it is well known in the art of mobile communication networks that authentication between the network and the mobile station requires the mobile station to access the DCK as noted in the paragraph and thus the network station wherein the mobile station resides would receive the authentication key), and wherein the mobile station is affiliated with a talkgroup associated with the first encryption key (page 50 paragraph 8 1st sentence wherein the first encryption key is the GCK).

15. As per claim 4, Roelofsen discloses the method of claim 1, wherein the third system device is any of a base station, a base site, and a TETRA site controller, wherein the step of forwarding the second encryption key to a third system device is triggered by a mobile station arriving at any of the base station, the base site, and the TETRA site controller, and wherein the mobile station is affiliated with a talkgroup associated with the first encryption key (the same rejection for claim 3 follows here, it is

Art Unit: 2132

well known in the art of mobile communication systems that a key needed to authenticate a mobile station would be sent to the base station as a particular mobile station arrives at a base station).

16. As per claim 6, Roelofsen discloses the method of claim 1, wherein the third encryption key is associated with the third system device (page 50 paragraph 6 wherein the third encryption key is the Common Cipher Key (CCK) and the third system device is the network station connected to the geographical area as understood in the art).

17. As per claim 7, Roelofsen discloses the method of claim 1, wherein the first encryption key is a group cipher key, the second encryption key is a modified group cipher key and the third encryption key is a common cipher key (page 50 paragraph 6, 8 and page 51 paragraph 2).

18. As per claim 8, Roelofsen discloses the method of claim 1, further comprising the step of communicating over an air interface by encrypting messages with the second encryption key (page 51 paragraph 2 wherein the second encryption key is the MGCK and is used to encrypt user group messages).

19. As per claim 10, Roelofsen discloses the method of claim 1 wherein the second system device is included in a first zone of devices:

encrypting the first encryption key with an interkey that is associated with the first zone of devices and at least a second zone of devices, yielding a first encrypted encryption key (page 52 column 1 lines 14-20);

Forwarding the first encrypted encryption key to a fourth system device included in the second zone of devices, wherein the fourth system device is other than a mobile

station and other than the first, second and third system devices (see claim 1 wherein the method and infrastructure is the same, now only for a visited network comprising the second zone);

Decrypting, by the fourth system device, the first encryption key into the first encryption key (this is an inherent step, since in order for the device to be able to use the key, it must be decrypted).

20. As per claim 11, Roelofsen discloses the method of claim 10, further comprising the steps of:

Generating, by the fourth system device, the second encryption key by combining the first encryption key with the third encryption key; and

Forwarding the second encryption key to a fifth system device included in the second zone of devices that is other than a mobile station and other than the first second, third and fourth system devices (see claim 1, the method applies the same only for a new network i.e. second zone).

21. As per claim 12, Roelofsen discloses the method of claim 11, wherein the second encryption key is encrypted with an intrakey associated only with the second zone of devices prior to being forwarded to the fifth system device (page 51 paragraph 1, wherein the keys are distributed by using session authentication keys derived from the session key for the second network/zone).

22. Claim 13 is rejected because it discloses the same subject matter as claim 6.

23. Claim 14 is rejected because it discloses the same subject matter as claim 7.

Art Unit: 2132

24. As per claim 15, Roelofsen discloses the method of claim 1, further comprising the steps of:

Encrypting the first encryption key with a key associated with a mobile station, yielding an encrypted mobile encryption key;

Forwarding the mobile encryption key to the mobile station (page 51 paragraph wherein the keys are transferred to the mobile station encrypted with the session authentication key unique to the mobile station).

25. As per claim 16, Roelofsen discloses the method of claim 15, further comprising the steps of:

Decrypting, by the mobile station, the encrypted mobile encryption key with the key associated with the mobile station, yielding the first encrypted key (this is inherent in the invention since the key is encrypted with a session authentication key associated with the mobile station, the mobile station must decrypt the first encrypted key);

Combining the first encryption key with a predetermined encryption key, yielding an air interface key (page 50 paragraph 5, wherein the predetermined key is the DCK);

Communicating over an air interface by encrypting messages with the air interface key (page 50 paragraph 5).

26. As per claim 17, Roelofsen discloses wherein the predetermined encryption key is a common cipher key (page 50 paragraph 6 and page 51 paragraph 2).

27. As per claim 18, Roelofsen discloses the method of claim 1, wherein the second device is included in a first zone of devices, the method further comprising the step of encrypting the first encryption key with an interkey associated with the first zone of

Art Unit: 2132

devices and at least a second zone of devices prior to the forwarding step, wherein the encrypted first encryption key is stored at the second system device (claim 1 and claim 10, wherein the session authentication key used to distribute the keys is a special key as used in the authentication of the user in the new zone).

28. As per claim 21, Roelofsen and Tiedemann disclose wherein the second system device contains a home location register associated with the first encryption key (see Tiedemann fig. 1).

Tiedemann is analogous art as applied to claim 1.

Motivation and obviousness for modifying Roelofsen to include a home location register would be well known by one of ordinary skill in the art. A home location register is a very common network element in wireless communication infrastructure and is necessary for verifying and enabling legitimate routing of calls and ensuring security in the network.

29. Claim 5 is rejected under 35 U.S.C. 103(a) as being unpatentable over Roelofsen in view of Tiedemann and further in view of Jackson (US Patent 6477387).

Roelofsen discloses the method of claim 1, wherein the third system device is any of a base station, a base site, and a TETRA site controller, but does not disclose wherein the step of forwarding the second encryption key to a third system device is triggered by a mobile station changing talkgroup affiliation while residing at any of the base station, the base site, and the TETRA site controller, and wherein the mobile station changes talkgroup affiliation to a talkgroup associated with the first encryption key.

Jackson discloses wherein an encryption key associated with a talkgroup is sent to a device when triggered by a change in talkgroup wherein the key is for the new talkgroup (column 14 lines 16-28).

Jackson is analogous art because it discloses a method for grouping communication units in a communication system.

It would have been obvious for one of ordinary skill in the art to modify Roelofsen to include a step of sending an encryption key for a new talkgroup when a mobile unit changes to the new talkgroup.

Motivation for one to modify Roelofsen as discussed above would have been for enabling secure communication for the user changing talkgroups, as discussed by Jackson in column 14 lines 22-26.

30. Claims 9 and 22 are rejected under 35 U.S.C. 103(a) as being unpatentable over Roelofsen in view of Tiedemann and further in view of Roelofsen ("Security Issues for TETRA Networks").

31. As per claim 9, Roelofsen ("TETRA Security") discloses the method of claim 1, but does not disclose wherein it further comprises the step of updating the first encryption key when an encryption period associated with the third encryption key expires.

Roelofsen ("Security Issues for TETRA Networks") does disclose the step of updating the first encryption key when an encryption period associated with the third encryption key expires (section 3.2).

Roelofsen is analogous art because it discloses methods of securing a TETRA network.

The author is the same for both articles and both specifically discuss security implementation in TETRA networks, so obviousness for one of ordinary skill in the art to combine and motivation to combine are inherent.

32. As per claim 22, Roelofsen ("Security Issues for TETRA Networks") discloses the method of claim 1, further comprising the step of updating the first encryption key when an encryption period associated with the first encryption key expires (section 3.2).

Obviousness and motivation to combine are applied as in claim 9.

33. Claims 19 and 20 are rejected under 35 U.S.C. 103(a) as being unpatentable over Roelofsen in view of Tiedemann and further in view of Marshall (US Patent 4888800).

34. As per claim 19, Roelofsen discloses the method of claim 18, but does not disclose it further comprising the step of acknowledging receipt of the first encryption key.

Marshall does disclose a method of acknowledging receipt of an encryption key (column 11 lines 19-40).

Marshall is analogous art because it is directed towards a method of distributing encryption keys.

It would have been obvious for one of ordinary skill in the art to modify Roelofsen to include the step of acknowledging the receipt of the encryption key.

Motivation for one to modify Roelofsen as discussed above would have been to ensure that the encryption key is received by the agent thus enabling secure communication in the future as is well known by one of ordinary skill in the art.

35. As per claim 20, Marshall discloses the step of claim 19, wherein the step of acknowledging comprises decrypting the first encryption key, and when the first encryption key is decrypted properly, generating an acknowledgment to be forwarded via an air traffic router to the first system device (column 11 lines 19-40).

Marshall is analogous art because it is directed towards a method of distributing encryption keys.

It would have been obvious for one of ordinary skill in the art to modify Roelofsen to include the step of acknowledging the receipt of the encryption key when the encryption key is decrypted properly.

Motivation for one to modify Roelofsen as discussed above would have been to ensure that the encryption key is properly received by the agent thus enabling secure communication in the future as is well known by one of ordinary skill in the art.

Conclusion

Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire **THREE MONTHS** from the mailing date of this action. In the event a first reply is filed within

TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Brandon S. Bludau whose telephone number is 571-272-3722. The examiner can normally be reached on Monday -Friday 8:00-5:30.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on 571-272-3799. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Brandon S Bludau

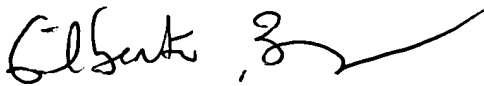
Application/Control Number: 09/785,849

Page 16

Art Unit: 2132

Examiner
Art Unit 2132

BB


GILBERTO BARRON JR
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100